

InterContinental Hotels Group (IHG) Notifies Guests of Payment Card Incident at IHG-Branded Franchise Hotel Locations in the Americas Region

NOTICE OF DATA BREACH

IHG values the relationship we have with our guests and understands the importance of protecting payment card data.

What Happened

Many IHG-branded locations are independently owned and operated franchises, and certain of these franchisee operated locations in the Americas were made aware by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at their locations. To ensure an efficient and effective response, IHG hired a leading cyber security firm on behalf of franchisees to coordinate an examination of the payment card processing systems of franchise hotel locations in the Americas region.

The investigation identified signs of the operation of malware designed to access payment card data from cards used onsite at front desks at certain IHG-branded franchise hotel locations between September 29, 2016 and December 29, 2016. Although there is no evidence of unauthorized access to payment card data after December 29, 2016, confirmation that the malware was eradicated did not occur until the properties were investigated in February and March 2017. Before this incident began, many IHG-branded franchise hotel locations had implemented IHG's Secure Payment Solution (SPS), a point-to-point encryption payment acceptance solution. Properties that had implemented SPS before September 29, 2016 were not affected. Many more properties implemented SPS after September 29, 2016, and the implementation of SPS ended the ability of the malware to find payment card data and, therefore, cards used at these locations after SPS implementation were not affected.

A list of affected IHG franchise locations and respective time frames, which may vary by location, is available [here](#).

What Information Was Involved

The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected hotel server. There is no indication that other guest information was affected.

What You Can Do

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

What We Are Doing

On behalf of franchisees, IHG has been working closely with the payment card networks as well as with the cyber security firm to confirm that the malware has been eradicated and evaluate ways for franchisees to enhance security measures. Law enforcement also has been notified.

For More Information

We regret any inconvenience this may have caused. If you have questions, and reside in the United States, please call 855-330-6367 from 8:00 a.m. to 8:00 p.m. ET, Monday to Friday. If you reside outside the United States, please call 800-290-9989 from 8:00 a.m. to 8:00 p.m. ET, Monday to Friday.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax

Phone: 1-800-685-1111

P.O. Box 740256

Atlanta, Georgia 30348

www.equifax.com

Experian

Phone: 888-397-3742

P.O. Box 9554

Allen, Texas 75013

www.experian.com

TransUnion

Phone: 800-916-8800

P.O. Box 2000

Chester, PA 19016

www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in California. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft